

**Statement by Derechos Digitales before the
Open-Ended Working Group on security of and in the use of
information and communications technologies (OEWG 2021-2025),**

Virtual informal dialogue with the Chair of the OEWG
6 December, 2023– J. Carlos Lara Gálvez

Mr Chair, distinguished colleagues,

Derechos Digitales is grateful for the opportunity to participate this meeting. We are a human rights organisation focused on the impact of the regulation, use and misuse of digital technologies on the enjoyment of human rights in Latin America. Based on that experience, we would like to contribute the following points to the Chair's question on the contribution of stakeholders to the implementation of recommendations in the second Annual Progress Report (APR).

Derechos Digitales conducts and supports digital security trainings and audits in Latin America, in partnership with local experts, directing efforts towards inclusivity. We have recently launched LaREDD, the Latin American Programme for digital defence and resilience, with a strong focus on threat response and the creation of technical capabilities in emerging organisations, and we have become part of the recently launched Global Network for Social Justice and Digital Resilience. These efforts, alongside our historic contribution to policy discussions, and our attention to national implementation of agreed norms, are the basis for our trust in the capacity of civil society and independent experts to contribute to the implementation of the recommendations from the APR.

On capacity-building, civil society can collaborate with States, regional organisations and relevant UN entities to align their capacity-building programmes with their human rights objectives and the 2021 principles for capacity-building. This includes promoting inclusivity, transparency, and respect for human rights in training programmes. Civil society can advocate for the integration of a gender perspective in capacity-building initiatives and encourage the development and sharing of tools that promote inclusivity in cybersecurity. Civil society can contribute to the UN Secretariat's recommended "mapping exercise" (p. 46) by sharing information about existing capacity-building programmes and initiatives. This can help identify gaps, avoid duplication, and promote coordination among stakeholders.

With regards to rules, norms and principles, states should consider civil society's capacity to offer expertise in the development of the checklist for the implementation of norms (p. 26), as they can help identify gaps in norms implementation by providing input for states and exchanging information in dedicated discussions. Civil society can be part of expert briefings to assist in ensuring that human rights and digital freedoms are adequately considered in drafting

processes. They can also run awareness efforts for different stakeholders about the importance of responsible state behaviour, to encourage states to uphold and implement the agreed norms and to make actors in cyberspace accountable.

Finally, on International Law, we support the convening of a “dedicated intersessional meeting” (p. 35), where non-governmental stakeholders could actively participate. Civil society can compile and analyse national views on how international law applies to the use of ICTs and how States’ positions and behaviours can be understood, for a comprehensive understanding of state perspectives and potential areas of consensus or contention. Civil society can engage with states to ensure that legal frameworks address human rights concerns and are consistent with established human rights standards and norms.

In summary, civil society involvement can provide diverse perspectives and contribute to the development of inclusive and human rights-focused outcomes.

Thank you, Chair.